

**Federal Tax Information Used by
Customer Satisfaction Survey
Contractors Needs to Be
Better Protected**

November 2000

Reference Number: 2001-10-012

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

November 28, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

A handwritten signature in black ink, reading "Pamela J. Gardiner".

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Federal Tax Information Used by Customer
Satisfaction Survey Contractors Needs to Be Better Protected

This report presents the results of our review of the vendor's and its subcontractors' security controls in protecting the integrity, confidentiality, and security of taxpayer data used in the Internal Revenue Service's (IRS) Customer Satisfaction Surveys.

In summary, we found that the vendor and its subcontractors can improve controls over federal tax information. While we found no evidence of improper disclosure of federal tax information, the vendor (who received just slightly less than 1 million taxpayer records in 1999) had not met all security requirements. We also determined the IRS had not conducted on-site security reviews of the vendor's and its subcontractors' facilities.

We recommended that the Director, Office of Program Evaluation and Risk Analysis, coordinate with the Office of Safeguards to develop a process to ensure that on-site security reviews of the vendor's and its subcontractors' facilities are conducted.¹ In addition, the Office of the Chief Communications and Liaison should evaluate the Office of Safeguards staffing and workload to ensure that proper oversight is given to private industry vendors.

¹ Since completion of our review, the responsibility for conducting and administering the customer satisfaction surveys has been transferred from the Office of Program Evaluation and Risk Analysis to the Organizational Performance Division.

IRS management agreed to take corrective action on all recommendations cited. Management's comments have been incorporated into the report where appropriate, and the full text of their comments is included as an appendix.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6500 if you have questions, or your staff may call Maurice S. Moody, Associate Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs), at (202) 622-8500.

**Federal Tax Information Used by Customer Satisfaction
Survey Contractors Needs to Be Better Protected**

Table of Contents

Executive Summary.....	Page i
Objective and Scope.....	Page 1
Background	Page 2
Results	Page 4
The Vendor and Its Subcontractors Need to Improve Controls Over Federal Tax Information	Page 5
The Internal Revenue Service Needs to Enhance Its Oversight Process of the Vendor and Its Subcontractors.....	Page 12
Conclusion.....	Page 16
Appendix I – Detailed Objective, Scope, and Methodology	Page 17
Appendix II – Major Contributors to This Report.....	Page 21
Appendix III – Report Distribution List.....	Page 22
Appendix IV – Data Flow Between the Vendor and Its Subcontractors	Page 23
Appendix V – Management’s Response to the Draft Report	Page 24

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

Executive Summary

This audit was performed as part of the Treasury Inspector General for Tax Administration's strategy to assess the relevance and reliability of the customer satisfaction performance measures relating to the Internal Revenue Service's (IRS) compliance with the Government Performance and Results Act of 1993 (GPRA).¹ The overall objective of this audit was to evaluate the integrity, confidentiality, and security of the taxpayer data in possession of the vendor and its subcontractors who conduct the surveys used to judge customer satisfaction.

The IRS balanced measurement system measures customer satisfaction, business results, and employee satisfaction. IRS management is using surveys as the measurement of taxpayers' opinions on service provided. To do this, the IRS contracted² with a vendor, at a cost of over \$4 million, to survey taxpayers who have had contact with the IRS.

As part of the survey process, the IRS provides sensitive but unclassified Federal Tax Information (FTI), such as taxpayers' names and addresses, to the vendor. Eight surveys³ involve FTI data that the vendor receives from the IRS and forwards to one of its subcontractors to generate the survey samples. In Calendar Year 1999, the vendor received slightly less than 1 million taxpayer records from the IRS to be processed for the customer satisfaction surveys. Due to the private and personal nature of the FTI, Internal Revenue Code § 6103⁴ requires the data to be protected from unauthorized disclosure. Unauthorized disclosure is subject to both civil and criminal penalties. Accordingly, the vendor and its subcontractors must establish security controls (safeguards) to protect FTI from unauthorized access and use.

Results

We reviewed six key security processes that covered physical and logical accesses, hiring and termination procedures, security awareness, and contingency planning. Three of the security processes were adequate, while the remaining three need to be improved. The vendor and its subcontractors were not meeting some of the security requirements in the

¹ Pub. L. No. 103-62, 107 Stat. 285.

² Through the Management, Organizational, and Business Improvement Services (MOBIS) contract.

³ The eight surveys are for the following IRS activities: Collection, Examination (Field and Office), Service Center-Examination, Exempt Programs-Examination, Exempt Organization-Examination, Exempt Programs-Determination, Exempt Organization-Determination, and Appeals.

⁴ 26 U.S.C. § 6103 (a) (1999).

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

contract and the IRS had not conducted a review of the safeguard measures employed by the vendor and its subcontractors. Although there were security weaknesses, the audit found no evidence of improper disclosure of FTI by the vendor or its subcontractors.

The Vendor and Its Subcontractors Need to Improve Controls Over Federal Tax Information

We identified three security controls that need to be enhanced to ensure the protection of FTI from unauthorized disclosure during the survey process.

- The minimum-security requirements were not being met for the Department of Defense “Class (C2): Controlled Access Protection” that the Department of the Treasury has adopted. Specifically, the vendor and the subcontractors did not maintain documentation on the security mechanisms within their computer systems. The vendor and its subcontractors did not have a control measure in place to determine who accesses protected information on the system. In addition, the vendor and one of the subcontractors did not have a security policy describing the system in terms of categories of data processed, users allowed access, and access rules between the users and the data.
- Physical controls need to be improved in handling and accounting for computer diskettes and tapes with FTI, storing FTI, and purging or destroying FTI after the customer satisfaction survey process is completed.
- A security awareness program is needed to ensure vendor employees have an understanding of security procedures required to protect FTI.

The Internal Revenue Service Needs to Enhance Its Oversight Process of the Vendor and Its Subcontractors

The IRS Office of Safeguards⁵ provides national oversight on contracts issued to federal, state, and local government agencies that have access to FTI. The Office of Safeguards applies the same oversight to private sector contractors who have access to FTI. The terms of the MOBIS contract permit the agency to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under the contract. This includes reviewing the security measures that the vendor and its subcontractors have taken to protect FTI. In accordance with the IRS Disclosure of Official Information Handbook, the Office of Safeguards is to conduct a review within 1 year of any contractors who are receiving FTI for the first time. Since the inception of the MOBIS contract, the Office of Safeguards

⁵ The Office of Safeguards reports to the Office of Governmental Liaison and Disclosure, which reports to Office of the Chief Communications and Liaison.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

has not performed an evaluation of the safeguard measures employed by the vendor and its subcontractors. Moreover, as of May 31, 2000, there were 1,211 open IRS contracts involving FTI or other disclosure issues that had been awarded since October 1, 1997. Of the 1,211 contracts, 1,022 (84 percent) qualified to be selected for a safeguard review.⁶ Of the 1,022 contracts only 47 (5 percent) had been reviewed by field Disclosure Officers or the National Office of Safeguards' staff.

Summary of Recommendations

We recommend that the Director, Office of Program Evaluation and Risk Analysis, coordinate with the Office of Safeguards to develop a process to ensure that on-site security reviews of the vendor's and subcontractors' facilities are conducted and safeguards are in place and functioning as stated in the contract.⁷ We further recommend that the Office of the Chief Communications and Liaison evaluate the Office of Safeguards staffing and workload to determine if enough focus is being given to private industry vendors to ensure that sensitive taxpayer data are properly safeguarded.

Management's Response: IRS management agreed to ensure that on-site security reviews of the vendor's and subcontractors' facilities are conducted. Also, the Chief Communications and Liaison will conduct a review of the entire Safeguard Office operation environment, including staffing and workload. Management's complete response is included as an appendix to the report.

⁶ The Office of Safeguards is required to perform a safeguard review on those contracts that are in effect for more than 6 months.

⁷ Since completion of our review, the responsibility for conducting and administering the customer satisfaction surveys has been transferred from the Office of Program Evaluation and Risk Analysis to the Organizational Performance Division.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

Objective and Scope

This audit was performed as part of the Treasury Inspector General for Tax Administration's strategy to assess the relevance and reliability of the Internal Revenue Service's (IRS) efforts to comply with the Government Performance and Results Act of 1993 (GPRA).¹

Certain security measures must be in place to protect taxpayer information.

The overall objective of this audit was to assess the security controls the vendor and its subcontractors have in place for protecting the integrity, confidentiality, and security of taxpayer data used in the IRS' Customer Satisfaction Surveys. The vendor and its subcontractors must meet IRS security requirements intended to safeguard taxpayer data from disclosure.

To identify the security requirements needed for protecting taxpayer data, we held discussions with representatives of the Office of Program Evaluation and Risk Analysis (OPERA) and met in Washington, D.C., with IRS staff from the Office of Disclosure and Safeguards and the Office of Procurement. We also met with the vendor and its subcontractors and conducted walk-throughs of their facilities located in Palo Alto, California, and Edina, Minnesota.

The scope of our work was limited to assessing security practices for physical and logical access controls over data, hiring and termination policies, security awareness, and contingency plans. We did not conduct any tests of the vendor's or its subcontractors' computer or telecommunication systems used to transfer data to and from each other. We conducted our fieldwork from April through June 2000 in accordance with *Government Auditing Standards*.

¹ Pub. L. No. 103-62, 107 Stat. 285.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are included in Appendix II.

Background

The GPRA mandated federal agencies to establish standards for measuring their performance and effectiveness. In this regard, the IRS established the Balanced Measurement System, consisting of three components: Employee Satisfaction, Customer Satisfaction, and Business Results.

The IRS has been contracting with a vendor since February 1998 to conduct customer satisfaction surveys.

To assess the customer satisfaction component, the IRS contracted with a vendor in February 1998, at a cost of over \$4 million, under the Management, Organizational, and Business Improvement Services (MOBIS) contract to conduct surveys of customers who had contact with the IRS (in person, over the telephone, or through correspondence). The surveys measure customer satisfaction in 11 major IRS activities. For eight of the surveys, the IRS provides the vendor with taxpayer data. These eight customer satisfaction surveys are listed in the table below.

Table 1: Customer Surveys for Which the Vendor Receives Taxpayer Data from the IRS

Examination	Appeals
Exempt Organizations-Examination	Exempt Organizations-Determination
Employee Plans-Examination	Employee Plans-Determination
Service Center-Examination	Collection

The vendor works with two subcontractors to select samples, administer the surveys, and tabulate and analyze the survey results.

The vendor receives taxpayer data from the IRS on various forms of media (tapes, cartridges, and diskettes). The vendor delivers the data to one of the subcontractors to generate the survey samples. Once a sample is

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

By definition, taxpayer information or federal tax information includes the name of the person who filed the return, his/her mailing address and taxpayer identifying number, or a combination thereof.

selected, the first subcontractor sends the sample back to the vendor using an electronic Bulletin Board System (BBS).² The vendor then forwards the information via a second BBS to the second subcontractor, who generates the documents sent to the taxpayers. After the taxpayers' responses to the surveys are received and tabulated, the second subcontractor sends the information back to the vendor using the second BBS. The vendor reviews and analyzes the data and provides the summary results to the OPERA. See Appendix IV for a flowchart of this process.

The IRS provides Federal Tax Information (FTI) to the vendor to conduct the surveys. FTI is defined as tax return and return information, which includes the name of a person who filed the return, the taxpayer's mailing address, and the taxpayer's identifying number. FTI is considered sensitive but unclassified information. Agencies, contractors, and state and local governments that receive FTI directly from the IRS must have adequate safeguards in place to protect the data received from unauthorized use, access, and disclosure.

The Department of the Treasury Security Manual (TD P 71-10) requires its bureaus to establish security-screening requirements for contract employees who have access to sensitive but unclassified information or data. The Internal Revenue Code (I.R.C.)³ stipulates how data should be protected and the penalties that can be imposed if the data are improperly accessed or disclosed.

As a condition for receiving returns or return information, I.R.C. § 6103(n) authorizes the IRS to impose compliance safeguard requirements upon contractors who handle FTI. I.R.C. § 6103 (p)(4) identifies safeguards that require the contractor to (1) maintain a permanent system of standardized

² The BBS is software set up on a computer that allows a user to download, upload, or access information from it.

³ 26 U.S.C. § 6103 (p)(4) (1999) and 26 U.S.C. §§ 7213 and 7431 (1997).

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

records; (2) maintain a secure area for storing returns or return information; (3) restrict access to the return or return information to authorized persons only; (4) provide other safeguards to protect the confidentiality of the returns and return information; (5) furnish a report to the Secretary⁴ which describes the safeguard measures established and used by the contractor; and (6) upon completion of use, send the return or return information to the Secretary or properly dispose of the data.

I.R.C. §§ 7213 and 7431 provide for criminal and civil penalty damages for unauthorized disclosure of returns and return information. In addition, punitive damages can result when gross negligence occurs resulting from a willful inspection or disclosure of a return or return information.

Furthermore, to ensure that FTI is adequately safeguarded from disclosure, the contractor's computer system that processes, stores, and transmits FTI must have computer access protection controls in place. The Department of the Treasury has adopted the Department of Defense's "Class (C2): Controlled Access Protection" minimum security requirements for computer access protection controls over systems handling FTI.

Results

We reviewed six key security processes that covered physical and logical accesses, hiring and termination procedures, security awareness, and contingency planning. Three of the security processes were adequate, while the remaining three need to be improved. The vendor and its subcontractors were not meeting some of the security requirements in the MOBIS contract and the IRS had not conducted a

⁴ Where the term Secretary is used, the IRS is the Secretary's designee.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

review of the safeguard measures employed by the vendor and its subcontractors. In Calendar Year 1999, the vendor received slightly less than 1 million records from the IRS to be processed for the customer satisfaction surveys. Even though there were security weaknesses, the audit found no evidence of improper disclosure of FTI by the vendor or its subcontractors.

The Vendor and Its Subcontractors Need to Improve Controls Over Federal Tax Information

We reviewed six security measures of controls to determine the effectiveness of protecting the confidentiality of FTI. The vendor and its subcontractors had established adequate controls in the following three areas:

- **Hiring policies** ensured that qualified and trustworthy individuals were hired. Hiring procedures include interviewing potential candidates, contacting prior employers, and performing reference checks.
- **Termination policies** ensured that terminated employees were denied access to operations and assets. Procedures include collecting card keys, changing locks, and removing individuals from the system.
- **Contingency plans** included procedures for restoring critical systems and applications and providing off-site storage locations for file and program back-ups.

The vendor and its subcontractors had not ensured that minimum-security requirements for Controlled Access Protection (logical controls) were in place. For example, a security plan was not documented describing the vendor's and subcontractors' computer systems, audit trails were not being used to show who accessed the FTI, and design and test documentation was not

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

available to describe how and what security mechanisms were initially tested and what the test results were. Under physical controls, diskettes with FTI were improperly handled, FTI was not properly stored, and FTI was not purged after the customer satisfaction survey process was completed. Lastly, there was no security awareness program ensuring that employees accessing FTI have an understanding of the manner in which FTI should be protected.

Minimum requirements under “Class (C2): Controlled Access Protection” are not being met

The MOBIS contract has disclosure clauses that require the vendor to provide minimum safeguards to prevent or detect improper access to or disclosure of FTI. Because of the extensive use of computers, the contract also contains specific language concerning the security to be provided for computer systems and personnel.

The vendor and its subcontractors have provided reasonable assurance of protecting FTI against unauthorized access, modification, disclosure, impairment, and loss. This was accomplished through establishing user identification codes, passwords, permissions, and profiles for those authorized to use the computer systems.

However, computer systems that are receiving, processing, storing, and transmitting FTI must have Class (C2) access protection controls according to the safeguard clause in the MOBIS contract. Under Class (C2), system users are individually accountable for their actions through login procedures, audits of security-relevant events, and resource isolation.⁵ Four elements are required to meet minimum Class (C2) requirements. The operating security features of the system must include a security policy, accountability,

⁵ Examples of resource isolation would be security settings or access privileges on directories and servers (e.g., read/write/execute) and firewalls used to prevent unauthorized access from outside the system network.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

assurance, and documentation. A security policy is a written document describing the system in terms of categories of data processed, users allowed access, and access rules between the users and the data.

Accountability requires maintaining access controls to ensure that unauthorized access does not go undetected and authorized users are accountable for their work.

Assurance requires that access controls and other security features are implemented and working when they are installed on the computer system.

Documentation requires describing how and what security mechanisms in the computer system were tested and determining the results.

The table below shows where the vendor and its subcontractors are not meeting all of the minimum requirements under “Class (C2): Controlled Access Protection.”

The vendor and its subcontractors are not meeting all “Class (C2): Controlled Access Protection” requirements in accordance with the MOBIS contract.

Table 2: Decision Table for Compliance with Class (C2) Requirements in the MOBIS Contract

Class (C2) Minimum Requirements	Vendor Meets Contract Requirements?	Subcontractor 1 Meets Contract Requirements?	Subcontractor 2 Meets Contract Requirements?
Security Policy	No	Yes	No
Accountability	No	No	No
Assurance	*	*	*
Documentation	No	No	No
* Audit did not test computer system to identify this requirement.			

Although the MOBIS contract identified the four elements to meet Class (C2) requirements, the contract did not provide a definition and purpose of each element. In early January 2000, the OPERA provided the vendor with *Tax Information Security Guidelines for Federal, State, and Local Agencies* (Publication 1075 - OMB No. 1545-0962). The OPERA received this information from the Procurement office, which recommended that it be used as a guide on data security. Prior to that, the vendor relied on industry information

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

gathered from its subcontractors' policies on data security.

Because the vendor and its subcontractors are not meeting Class (C2) requirements, the risk of FTI being unaccounted for is increased, which could invalidate the customer satisfaction survey process. For example, if an integrity component (data validation) within the computer system is not functioning there is a risk that FTI could be unaccounted for during processing, thus invalidating the customer satisfaction survey results.

Physical controls need to be enhanced to ensure that FTI is adequately protected from unauthorized disclosure

Physical controls can be used as a safeguard to prevent or detect unauthorized access. As a condition of receiving FTI, the receiver must show, to the satisfaction of the IRS, its ability to protect the confidentiality of that information.

The vendor and its subcontractors implemented some physical safeguard measures to ensure that FTI was protected. For example, visitors are controlled at the front entrance of the office, the doors to the office are locked during non-duty hours, and only authorized individuals keep control over keys and combinations. However, there are areas where physical controls could be enhanced, particularly at the vendor's office, as the vendor had sub-let space to a third party who had access to areas where FTI was used. For example, computer diskettes and tapes containing FTI were not always properly stored and data had not been purged from all systems when required.

The vendor did not properly control IRS diskettes with FTI.

Diskettes containing FTI were not always properly stored.

The IRS submits FTI to the vendor on computer diskettes for one of the customer satisfaction surveys. However, the FTI was not accounted for or secured in a locked container when the vendor received it. The diskettes remained on top of an employee's desk in an unlocked room. Additionally, the IRS had not requested

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

the return of the diskettes until we brought it to the vendor's attention. The vendor's employee then contacted the IRS for disposition instructions and the diskettes were subsequently returned.

According to Publication 1075, authorized employees of the contractor must be responsible for securing magnetic media before, during, and after processing. Also, proper acknowledgment must be signed and returned to the IRS, and inventory records must be maintained for control and accountability.

The IRS employee responsible for sending the diskettes to the vendor did not require the vendor to return them. The return of the diskettes was not considered a priority since the IRS had the information on its database.

The risk of unauthorized personnel gaining access will increase when unsecured FTI is exposed in an open area. This could result in unauthorized disclosure of taxpayer information.

Three IRS tapes misplaced since November 1999 were subsequently found commingled with data of another client of the subcontractor.

Some computer tapes were misplaced.

One of the subcontractors received IRS tapes and cartridges from the vendor for processing. The subcontractor maintained the tapes and cartridges in a small safe within the locked storage room that contains other clients' data as well. The safe was not large enough to hold all IRS tapes and cartridges. As a result, some tapes were stacked on top of the safe. During our site visit on February 29, 2000, the vendor informed us that three IRS tapes were unaccounted for since November 1999. We asked the vendor to follow up on the three tapes. They were subsequently found commingled with data of another client of the subcontractor.

According to Publication 1075, FTI should be kept separate from other information to the maximum extent possible. In situations where it is impractical, the file should be labeled to indicate FTI is included and the file should be safeguarded. In addition, management must determine the type of space, container, and other security needs on a case by case basis.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

*The vendor has yet to purge
FTI from its computer system.*

Although the vendor received Publication 1075 from the IRS, its subcontractor was unaware that this document existed. Lacking this guidance, the subcontractor relied on a security document that it developed internally.

Confidentiality of FTI can be compromised when the tapes are not properly accounted for. The risk of inadvertent disclosure increases when FTI is commingled with the other subcontractor's client data. This could result in providing FTI to unauthorized individuals.

Upon completion of use, the vendor did not ensure that the FTI was deleted from its system.

The vendor processes FTI on its computer system for 8 of the 11 customer satisfaction surveys (see Table 1). After the FTI has been completely processed, the information remains on the vendor's system. The vendor does not purge the FTI when the customer satisfaction survey work is completed and the results are returned to the IRS.

In accordance with the MOBIS contract, the vendor must certify that the data processed during the performance of the contract are completely purged from all data storage components of the computer facility. In addition, the vendor is to retain no output at the time the IRS work is completed. If immediate purging of all data storage components is not possible, the contractor is to certify that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosure.

The vendor indicated that the information is being maintained on its system indefinitely in case the IRS requests additional information for analysis. Therefore, care must be taken to ensure the data are secured or the vendor could be subject to civil damages if unauthorized disclosure of FTI should occur. The data should be deleted as soon as the IRS and the vendor determine they are no longer needed.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

The vendor and its subcontractors need to establish a security awareness program

The vendor and its subcontractors should ensure that their employees are made aware of the importance of handling FTI and the legal and business reasons for maintaining its integrity and confidentiality. However, the vendor and its subcontractors did not fully develop a security awareness program, as required by Publication 1075.

We interviewed three employees at the vendor's facility and determined that they had not received any training on security awareness. However, the vendor does communicate security measures periodically to employees via e-mail. In addition, we observed that the vendor posted security reminder signs on the exit doors throughout the office.

Both subcontractors indicated that they did not have a formalized security awareness program. One subcontractor had security measures outlined in its security summary, but there was no documentation that employees received this policy statement and acknowledged it. The other subcontractor stated that it communicated security procedures to employees at staff meetings; however, the subcontractor did not have documentation available to support this.

According to Publication 1075, contractor employees should certify that they understand security procedures requiring their awareness and compliance before being granted access to FTI. Annually, employees should be re-certified to maintain their authorization to access FTI and be advised of provisions referring to unauthorized disclosure of FTI, unauthorized inspection of returns or return information, and civil penalties associated with unauthorized disclosure of returns or return information.

The vendor and its subcontractors used their own internally developed data security procedures through the end of Calendar Year 1999. In January 2000, the OPERA provided the vendor with Publication 1075 to be used as a guide to meet the security requirements

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

stated in the MOBIS contract. However, the subcontractors continued to use their own security procedures because they were not made aware of Publication 1075 by the vendor or the IRS.

In the absence of effective security awareness procedures, misuse of taxpayer information by employees could result in employees being at risk of unauthorized disclosure and subject to civil penalties. In addition, the risk of having invalid customer satisfaction survey results could occur from authorized employees tampering with or destroying FTI.

The Internal Revenue Service Needs to Enhance Its Oversight Process of the Vendor and Its Subcontractors

The Office of Safeguards, a subgroup under the Office of Governmental Liaison and Disclosure, serves as the IRS Safeguard Program administrator that provides national oversight to the districts, service centers, and headquarters operations on disclosure provisions set forth in the I.R.C. and the Privacy Act of 1974.⁶ In addition, the Office of Safeguards serves as the liaison to IRS contractors and federal and state agencies that are recipients of FTI.

The Office of Safeguards administers a Safeguard Review Program for all recipients of FTI. This includes conducting comprehensive on-site safeguard reviews and issuing reports of findings and recommendations for those federal and state agencies and IRS contractors that receive FTI.

In accordance with the terms of the MOBIS contract and I.R.C. § 6103(h), the IRS may send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided

⁶ I.R.C. § 6103 and Privacy Act of 1974 5 U.S.C. § 552a, as amended.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

for the performance of any work under the MOBIS contract. IRS procedures require that agencies receiving FTI for the first time must be reviewed within 1 year of initial receipt of the FTI. Further, the IRS holds private sector contractors to the same standards. The Office of Safeguards has not performed an evaluation of the safeguard measures employed by the vendor and its subcontractors.

Moreover, as of May 31, 2000, there were 1,211 open contracts with known disclosure issues that had been awarded since October 1, 1997.⁷ Of the 1,211 contracts, 1,022 (84 percent) qualified to be selected for a safeguard review.⁸ Of the 1,022 contracts, only 47 (5 percent) had been reviewed by the field Office Disclosure Officers or the National Office of Safeguards' staff.

The Office of Safeguards has five enforcement specialists on staff at the National Headquarters who perform safeguard reviews. However, none of the five enforcement specialists has the technical computer background to determine whether a contractor met Class (C2) requirements. We were informed that the Office of Safeguards had a computer specialist on staff; however, the employee left to take a higher position (doing the same work) at another federal agency. The Office of Safeguards further stated that a lack of funding has prevented it from hiring additional staff.

In addition to the Office of Safeguards, there are 43 Disclosure Officers in the field (33 districts and 10 service centers) who perform safeguard reviews if there is a contract in effect in their area. The safeguard reviews are performed as a function of the Disclosure Officer's collateral duties and are not considered a priority relative to their other workload.

⁷ The Procurement Office provided statistics on open contracts with disclosure issues; the Office of the Treasury Inspector General for Tax Administration has not audited these figures.

⁸ The Office of Safeguards will perform a safeguard review on those contracts that are in effect for more than 6 months.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

A new RFQ was finalized in April 2000.

Generally, each Disclosure Officer is asked to conduct at least one safeguard review per year. Even with this supplemental help, there is little chance that most contracts involving taxpayer information will be reviewed.

There is a risk of unauthorized disclosure of FTI when the vendor and its subcontractors have not implemented adequate safeguard measures to protect FTI. The risk increases when the IRS does not make an on-site visit to evaluate first hand what measures have been employed.

The current MOBIS contract is due to expire September 30, 2000. In April 2000, the IRS finalized a new request for quotation (RFQ) for the customer surveys, which included a clarification of Class (C2) and physical security requirements and additional requirements for the contractor to comply with under the MOBIS contract.

In accordance with I.R.C. § 6103 (p)(4)(E), contractors are now required to file a Safeguard Procedures Report (SPR), which describes how FTI is being protected from unauthorized disclosure. Thereafter, the contractor must file an annual Safeguard Activity Report. This report advises the IRS of changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the contractor's safeguard procedures, summarizes the contractor's current efforts to ensure the confidentiality of the FTI, and certifies that the contractor is protecting FTI pursuant to I.R.C. § 6103 (p) and the contractor's own security requirements.

Recommendations

1. The Director, OPERA, should coordinate with the Office of Safeguards to develop a process to ensure that on-site security reviews of the vendor's and its subcontractors' facilities are conducted and safeguards are in place and functioning as stated in the MOBIS contract.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

Management's Response: IRS management has included requirements in their new customer satisfaction contract requiring vendors to be capable of meeting Class (C2) level standards for physical and computer security. Included in these standards is the requirement that contractors must file an initial Safeguard Procedures Report (SPR) which describes how FTI is being protected from unauthorized disclosure and follow up with a Safeguard Activity Report on an annual basis. In addition, IRS management is requiring security clearances for employees who have access to tax return data. As a result, contractor security upgrades are being made to meet these Class (C2) requirements, and a process is being developed with the Office of Safeguards to perform inspections of vendors and subcontractors.

2. The Office of the Chief Communications and Liaison should evaluate the Office of Safeguards staffing and workload to ensure that proper oversight is given to private industry vendors to determine if they are adequately protecting the significant amounts of sensitive taxpayer data they receive from the IRS.

Management's Response: IRS management agrees that the IRS must do security reviews to ensure that security requirements are met. The Organizational Performance Division⁹ will work with the Office of Safeguards to ensure that the survey contractors' handling of FTI meets the security requirements imposed by the IRS. In addition, the Chief Communications and Liaison will conduct a review of the entire Safeguard Office operation environment including staffing and workload.

⁹ Since completion of our review, the responsibility for conducting and administering the customer satisfaction survey has been transferred from the Office of Program Evaluation and Risk Analysis to the Organizational Performance Division.

Conclusion

The vendor and its subcontractors have not complied with all security requirements stated in the MOBIS contract. As a result, there is an increased risk for unauthorized disclosure of FTI. Although the IRS has taken the action with the new RFQ to clarify security requirements that the vendor and its subcontractors must implement, the IRS has not provided sufficient oversight of the vendor and its subcontractors to ensure that adequate safeguards are in place to protect FTI.

Detailed Objective, Scope, and Methodology

Our overall objective was to determine if the vendor and each subcontractor had adequate controls in place to protect the integrity, confidentiality, and security of taxpayer data.

To accomplish this, we conducted the following tests:

- I. Determined the data security requirements of the MOBIS (Management, Organizational, and Business Improvement Services) contract and modifications entered into by the vendor and the Internal Revenue Service (IRS).
 - A. Determined the expectation of the Contracting Officer to include the disclosure clause regarding safeguarding of taxpayer information in the possession of the contractor.
 - B. Determined the process for a contractor to be certified as Class (C2) compliant.
 - C. Identified amendments made to the MOBIS contract agreement.
 - D. Determined the status and contents of the request for quotation.
- II. Determined if the vendor and each subcontractor had a sound, security management structure established.
 - A. Determined if the vendor and each subcontractor had a security policy.
 - 1. Reviewed security plans for the vendor and each subcontractor to determine if the plan had been documented and approved.
 - 2. Determined whether the security plans for the vendor and each subcontractor covered the requirements prescribed by Office of Management and Budget Circular A-130.
 - 3. Reviewed organization charts and job descriptions to determine if an information system security manager had been appointed at an overall level and at appropriate subordinate levels.
 - 4. Reviewed documentation supporting or evaluating a security awareness program.
 - 5. Reviewed security plans to determine if they clearly identified owners of computer-related resources and responsibility for managing access to computer resources.
 - B. Determined if system owners and users were aware of the security policies.

**Federal Tax Information Used by Customer Satisfaction
Survey Contractors Needs to Be Better Protected**

1. Reviewed the documentation supporting or evaluating security awareness programs.
 2. Interviewed system owners and users and determined what training they have received and if they were aware of their security-related responsibilities.
 3. Reviewed memoranda, electronic mail files, and other policy distribution mechanisms.
- C. Determined if incident response capability had been implemented.
1. Interviewed security managers.
 2. Reviewed documentation supporting incident handling activities.
- D. Determined if system owners identified authorized users and if users were authorized to access the vendor's and subcontractors' systems.
- E. Reviewed policies and procedures on access authorization.
1. Interviewed security or systems administrators to determine their policy and procedures on access authorization.
 2. Determined how passwords are issued to users and how they are secured.
 3. Determined how often passwords are changed.
 4. Determined the maximum number of allowed repeated attempts to log on using an invalid password.
- F. Determined if the vendor and each subcontractor monitored access, investigated apparent security violations, and took appropriate remedial action.
1. Determined if audit trail features were available and used.
 2. Reviewed policies and procedures on security violations and any available security violation reports.
 3. Determined if suspicious access activities were investigated and appropriate action was taken.
- G. Determined if adequate controls had been established at the vendor and each subcontractor in processing taxpayer data through the Bulletin Board System.
1. Interviewed management to gain an understanding of the process.
 2. Prepared a flowchart of the processing of taxpayer data for each of the 11 customer satisfaction surveys.

**Federal Tax Information Used by Customer Satisfaction
Survey Contractors Needs to Be Better Protected**

- H. Determined if the vendor and each subcontractor had adequate physical controls established.
 - 1. Interviewed management for policy and procedures on physical controls.
 - 2. Determined whether visitors were controlled within the office.
 - 3. Reviewed diagrams of the offices' physical layout to determine if controls were in place.
 - 4. Conducted a walk-through of the vendor's and each subcontractor's facility and identified any weaknesses in controls.
 - 5. Observed entries and exits from offices.
 - 6. Reviewed secured area where tapes/cartridges are stored.
 - a) Reconciled taxpayer media (there were 306 AIMS Tapes) that the vendor received from the IRS with those tapes that were returned to the IRS to determine if all tapes were accounted for during the period January 1998 through March 2000.
 - b) Identified the number of tapes outstanding that have not been returned to the IRS.
 - c) Identified the total number of records on each tape.
- III. Determined if the vendor and each subcontractor had a sound administrative policy for hiring and terminating employees.
 - A. Reviewed procedures for hiring and terminating employees.
 - B. Interviewed the Human Resource Manager or equivalent to describe the hiring and termination processes.
 - 1. Reviewed the methodology used to hire employees.
 - 2. Reviewed the methodology used to terminate employees.
 - C. Identified training that employees receive once hired.
 - D. Reviewed documentation that employees were expected to sign when hired or terminated relating to confidentiality of taxpayer data.
 - E. Reviewed procedures to remove terminated employees from the vendor's and its subcontractors' computer systems (password, profile, etc.).
- IV. Determined if the vendor and each subcontractor had implemented a contingency plan.
 - A. Interviewed senior management.

**Federal Tax Information Used by Customer Satisfaction
Survey Contractors Needs to Be Better Protected**

- B. Reviewed the contingency plan and determined if it had been tested.
- C. Determined if an off-site storage facility was available.
- D. Determined if staff had been trained to respond to emergency situations.
- E. Reviewed policies and procedures for backing up data.

Major Contributors to This Report

Maurice S. Moody, Associate Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs)

John R. Wright, Director

Kevin Riley, Audit Manager

Ken Henderson, Senior Auditor

David Robben, Senior Auditor

Tom Burroughs, Auditor

Lynn Ross, Auditor

**Federal Tax Information Used by Customer Satisfaction
Survey Contractors Needs to Be Better Protected**

Appendix III

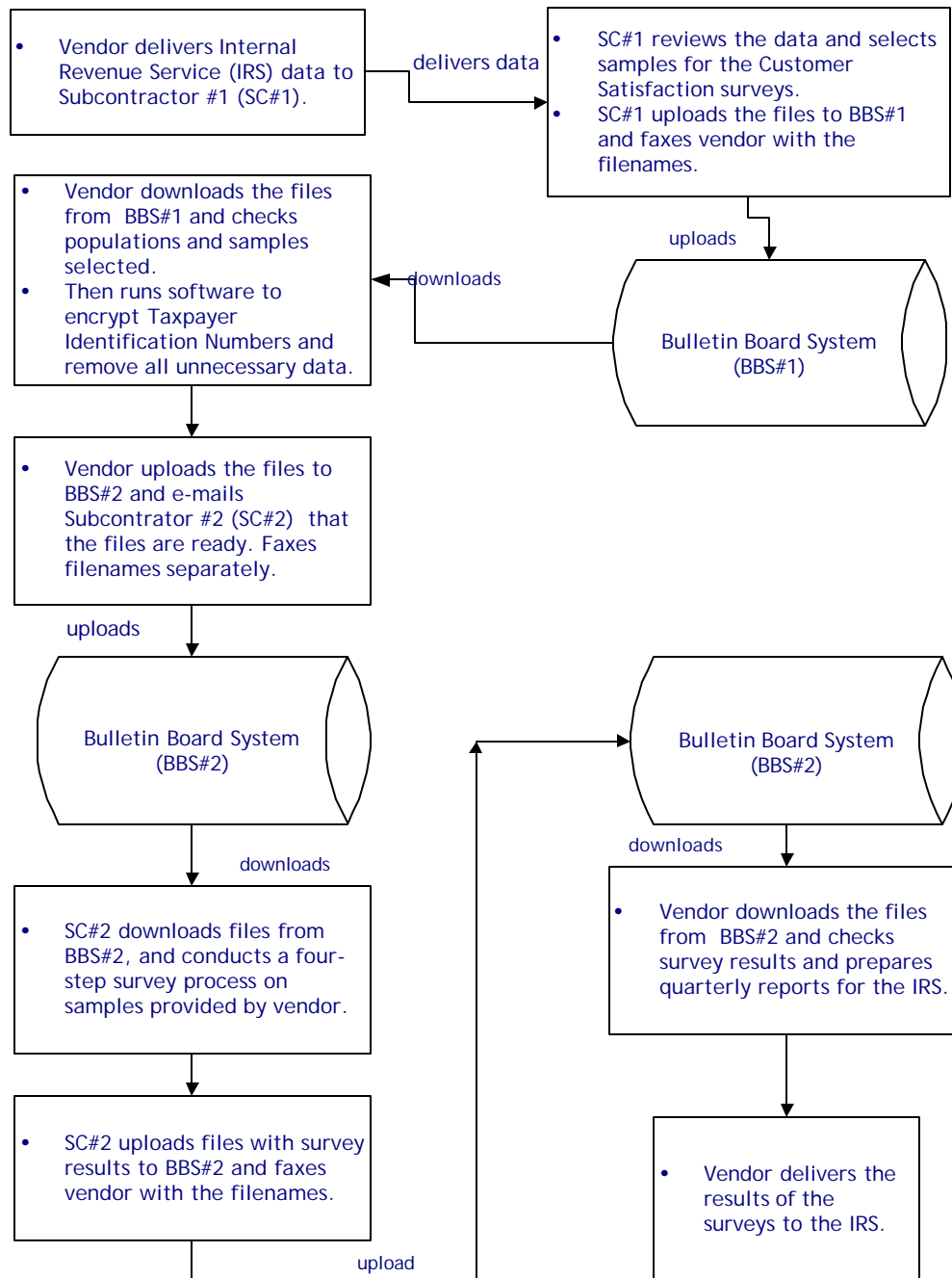
Report Distribution List

Deputy Commissioner Operations C:DO
Office of Management Controls M:CFO:A:M
Chief Counsel CC
Director, Governmental Liaison and Disclosure CL
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis M:O
Director, Organizational Performance Division OP
Director, Procurement A:P
National Taxpayer Advocate C:TA
Audit Liaisons:
 Director, Governmental Liaison and Disclosure CL
 Director, Office of Program Evaluation and Risk Analysis M:O

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

Appendix IV

Data Flow Between the Vendor and Its Subcontractors



**Federal Tax Information Used by Customer Satisfaction
Survey Contractors Needs to Be Better Protected**

Appendix V

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

October 25, 2000



MEMORANDUM FOR TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

FROM: David A. Mader 
Assistant Deputy Commissioner Operations

SUBJECT: Draft Audit Report – Federal Tax Information (FTI) Used by
Customer Satisfaction Survey Contractors Needs to be Better
Protected (Audit No. 2000100176)

Thank you for the opportunity to respond to your draft report entitled "Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to be Better Protected." The review assessed the security and handling of federal tax information by our customer satisfaction survey vendors and their subcontractors.

We were pleased your review found no evidence of improper disclosure of federal tax information. Your report did, however, conclude that the vendor and its subcontractors did not comply with all the security requirements stated in the MOBIS contract. As a result of your finding, the vendor has taken the necessary steps to be fully compliant with those security requirements. Attached is a more detailed description of the actions undertaken by the vendor.

As you know, in the redesigned National Headquarters Office, the responsibility for conducting and administering the customer satisfaction survey effort has been transferred to the new Organizational Performance Division (OPD). OPD will coordinate with the Office of Safeguards to develop a process to perform inspections of our survey contractors and subcontractors to ensure all security requirements are met.

In addition, the Office of Safeguards, which was recently realigned to Communications and Liaison, is planning to undertake a thorough review of our safeguard function, including contractor use of taxpayer data. As you recommend, the review will evaluate workload, staffing and policy issues to develop a comprehensive plan of action for ensuring sensitive taxpayer data is properly protected.

We look forward to working with you in the future to improve the quality of our Customer Satisfaction Survey effort. Our comments on the specific findings and recommendations in your report are as follows.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

2

IDENTITY OF RECOMMENDATION #1

The Director, OPERA, should coordinate with the Office of Safeguards to develop a process to ensure that on-site security reviews of the vendor's and its subcontractors' facilities are conducted and safeguards are in place and functioning as stated in the MOBIS contract.

ASSESSMENT OF CAUSE:

Although the MOBIS contract identified the four elements needed to meet Class (C2) requirements, the contract did not provide a definition and purpose for each element. The IRS Procurement Office recommended that Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies* be used as a guide on data security. OPERA provided the vendor with this publication in January 2000. Prior to that, the vendor relied on industry information relating to data security.

We believe OPERA acted responsibly and took reasonable steps to ensure the security of taxpayer data. In all, OPERA staff made a half dozen visits to the vendor and its subcontractors' facilities during the contract period. While not experts in security, OPERA trips were made to ensure contractor adherence to all contract requirements, specifically with the security of tax information in mind. Thankfully, your report did not reveal any instances of improper disclosure of Federal Tax Information (FTI).

CORRECTIVE ACTIONS:

While, the contract referred to in this report expired on September 30, 2000, our new customer satisfaction contract also requires the vendors to be capable of meeting Class (C2) level standards for physical and computer security. Included in these standards is the requirement that contractors must file an initial Safeguard Procedures Report (SPR) which describes how FTI is being protected from unauthorized disclosure, and follow up with a Safeguard Activity Report on an annual basis. We are also requiring security clearances for vendor employees who have access to tax return data. As a result, contractor security upgrades are being made to meet these Class (C2) requirements, and a process is being developed with the Office of Safeguards to perform inspections of our vendors and subcontractors.

IMPLEMENTATION DATE (S):

Effective December 1, 2000

RESPONSIBLE OFFICIAL(S):

Director, Organizational Performance Division
Chief Communications and Liaison

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

CORRECTIVE ACTION MONITORING PLAN

The Organizational Performance Division, which oversees the contract with the vendors, and the Chief Communications and Liaison, who oversees the Office of Safeguards, will monitor these changes.

IDENTITY OF RECOMMENDATION #2

The Office of the Chief Communications and Liaison should evaluate the Office of Safeguards staffing and workload to ensure that proper oversight is given to private industry vendors to determine if they are adequately protecting the significant amounts of sensitive taxpayer data they receive from the IRS.

ASSESSMENT OF CAUSE:

The report addresses concerns for taxpayer confidentiality and safeguard reviews in light of existing staffing and Internal Revenue Manual directives.

CORRECTIVE ACTIONS:

While the Office of Safeguards is not specifically required to conduct security reviews of private sector vendors, we agree that the Service must do these reviews need to ensure that security requirements are met. The Organizational Performance Division will work with the Office of Safeguards to ensure that the survey contractors' handling of FTI meets the security requirements imposed by the IRS. In addition, the Chief Communications and Liaison will conduct a review of the entire Safeguard Office operation environment including staffing and workload.

IMPLEMENTATION DATE (S):

December 1, 2000

RESPONSIBLE OFFICIAL (S):

Chief Communications and Liaison
Director, Organizational Performance Division

CORRECTIVE ACTION MONITORING PLAN

The Organizational Performance Division, which oversees the contract with the vendors, and the Chief Communications and Liaison, who oversees the Office of Safeguards, will monitor these changes.

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

Attachment

Pacific Consulting Group (PCG) implemented improvement mechanisms in four main areas to more fully protect Federal Taxpayer Information (FTI) received from the IRS.

The main areas are:

(1) improvements to reduce reliance on subcontractors for FTI-related work; (2) improvements to physical security; (3) improvements to computer system security; and (4) development of a formal Security Awareness Program.

Reducing Reliance on Subcontractors with Access to FTI

To reduce reliance on subcontractors for FTI-related work, PCG is bringing “in-house” the functions related to database cleaning and sampling which were originally handled by a subcontractor. These tasks will be protected – both physically and computer-wise – as outlined below.

Under the original contract, a second subcontractor handled the survey mailing tasks. That work is now being transferred to The Gallup Organization, which is another IRS Customer Satisfaction Survey vendor (not a subcontractor to PCG).

Improving Physical Security

To improve physical security, PCG is creating a restricted-access, secured area within its offices – the Analysis Suite – to prevent undetected entry by unauthorized persons during non-duty hours. All work with FTI will occur in the Analysis Suite. New physical security mechanisms include:

- entrance to the Analysis Suite limited to PCG staff with authorized access;
- off-duty hours protection by a UL-approved electronic intrusion system, with door sensors, glass-break sensors, and motion detectors;
- access to the Analysis Suite controlled by a UL-approved access-control system that provides regular monitoring reports of who enters or exits the room and when;
- inventory log of access cards issued;
- exterior windows in the Analysis Suite made of security glass; and
- background investigations for those staff authorized for access to FTI

Specific to the TIGTA audit report, as part of improving *physical controls*, PCG will:

- label all tapes and cartridges containing FTI as instructed by the IRS;
- ship all FTI between PCG and the mail house using Federal Express (with signature required on receipt);
- improve object reuse requirements, including using Windows NT 4.0 capabilities to reinitialize memory before use;
- store all materials (e.g., tapes, cartridges, paper) containing FTI in the Analysis Suite;

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

- meet periodically with IRS staff to identify which files containing FTI will not be needed for future analysis and should be purged and destroyed, and then purge and destroy them appropriately, with proper notification to the IRS; and
- shred computer tapes & cartridges containing FTI to IRS specifications by an outside shredding and disposal firm (along with the paper materials).

Improving Computer Security

To improve computer security, PCG will also change its corporate computer network to meet C2 requirements. This will include:

- adding a second domain – the IRS domain – accessible only by authorized staff;
- using Windows NT 4.0 with Service Pack 6a and the C2 Update on the IRS server and workstations used by authorized staff;
- using basic access control and account lock-out features of Windows NT 4.0;
- tightening System Administrator access requirements and controls;
- removing modems from workstations in the Analysis Suite;
- installing and using the appropriate hardware/software to periodically validate the correct operation of the hardware and firmware elements of the Analysis Suite and the IRS domain server; and
- testing the security mechanisms of the IRS domain server to ensure that they work as claimed in system documentation.

Specific to the TIGTA audit report, as part of *installing a new computer system*, PCG will also:

- develop full documentation on the security mechanisms within that system, including protection mechanisms provided by the IRS domain server, guidelines on use, and how they interact with one another; functions and privileges to be controlled to protect FTI; and system security test plan, testing procedures, and results of periodic system tests;
- implement control measures to determine who accesses protected information on the system, including using Windows NT 4.0 event logs to record security-related events; and
- develop and communicate a security policy that describes the system in terms of categories of data processed, users allowed access, and access rules between the users and the data.

Developing a Formal Security Awareness Program

Specific to the TIGTA audit report, PCG will implement the following additional education mechanisms to ensure that all staff are made aware of what FTI is and how it is to be safeguarded. PCG will:

- include a special appendix in the PCG Staff Handbook that outlines the firm's Data Security Program for Safeguarding FTI and a separate statement of PCG's Data Security Policy; and

Federal Tax Information Used by Customer Satisfaction Survey Contractors Needs to Be Better Protected

- hold an annual Data Safeguards meeting each year with staff who are authorized access to FTI. Discussion items will include: (1) the confidentiality provisions of the IRC, (2) the definition tax return and tax return information, (3) the civil and criminal sanctions for unauthorized inspection or disclosure, and (4) the company's data safeguarding procedures.